

WEST[Help](#)[Logout](#)[Interrupt](#)[Main Menu](#)[Search Form](#)[Posting Counts](#)[Show 8 Numbers](#)[Edit 8 Numbers](#)[Preferences](#)[Cases](#)**Search Results -**

Terms	Documents
L1 and (healthcare or health adj car\$3 or hospital or pharmac\$3 or food drug administration or FDA)	4

Database: US Patents Full-Text Database
US Pre-Grant Publication Full-Text Database
JPO Abstracts Database
EPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search: L10 Refine Search

Recall Text Clear

Search History

DATE: Wednesday, July 31, 2002 [Printable Copy](#) [Create Case](#)

Set Name Query

side by side

Hit Count Set Name

result set

DB=USPT; PLUR=YES; OP=ADJ

<u>L10</u>	L1 and (healthcare or health adj car\$3 or hospital or pharmac\$3 or food drug administration or FDA)	4	<u>L10</u>
<u>L9</u>	L1 and (healthcare or healt adj car\$3 or hospital or pharmac\$3 or food drug administration or FDA)	4	<u>L9</u>
<u>L8</u>	l1 and (healthcare or healt adj car\$3 or hospital or service adj provid\$3 or pharmac\$3 or food drug administration or FDA)	12	<u>L8</u>
<u>L7</u>	l6 and (healthcare or healt adj car\$3 or hospital or service adj provid\$3 or pharmac\$3 or drug)	4	<u>L7</u>
<u>L6</u>	L5 and (warn\$3 or recall\$3 or safety advisory)	4	<u>L6</u>
<u>L5</u>	L4 and third party	6	<u>L5</u>
<u>L4</u>	l1 and (broadcast\$3 or transfer\$4 or transmit\$4 or send\$3) near5 (document or file or data or information) same (consumer or customer or client)	20	<u>L4</u>
<u>L3</u>	L1 and (broadcast\$3 or transfer\$4 or transmit\$4 or send\$3) near5 (document or file or data or information) same (consumer or customer or client) same third party	0	<u>L3</u>
<u>L2</u>	L1 and (broadcast\$3 or transfer\$4 or transmit\$4 or send\$3) near5 (document or file or data or information) same (consumer or customer or client) same third adj party	0	<u>L2</u>
<u>L1</u>	(5619648 or 5623656 or 5627764 or 5636346 or 5649186 or 5678002 or 5691917 or 5694546 or 5696965 or 5710884 or 5717923 or 5722418 or 5724521 or 5724567 or 5732212 or 5740549 or 5745669 or 5748877 or 5754938 or 5754939 or 5758257 or 5764898 or 5768508 or 5774170 or 5778187 or 5790798 or 5802253 or 5802518 or 5805897 or 5828837 or 5835087 or 5848271 or 5848396 or 5850520 or 5854828 or 5855018 or 5862322 or 5867714 or 5867799 or 5870724).pn.	40	<u>L1</u>

END OF SEARCH HISTORY

WEST

Generate Collection

Print

L5: Entry 5 of 6

File: USPT

DOCUMENT-IDENTIFIER: US 5754938 A

TITLE: Pseudonymous server for system for customized electronic identification of desirable objects

US PATENT NO. (1):5754938Abstract Text (1):

This invention relates to customized electronic identification of desirable objects, such as news articles, in an electronic media environment, and in particular to a system that automatically constructs both a "target profile" for each target object in the electronic media based, for example, on the frequency with which each word appears in an article relative to its overall frequency of use in all articles, as well as a "target profile interest summary" for each user, which target profile interest summary describes the user's interest level in various types of target objects. The system then evaluates the target profiles against the users' target profile interest summaries to generate a user-customized rank ordered listing of target objects most likely to be of interest to each user so that the user can select from among these potentially relevant target objects, which were automatically selected by this system from the plethora of target objects that are profiled on the electronic media. Users' target profile interest summaries can be used to efficiently organize the distribution of information in a large scale system consisting of many users interconnected by means of a communication network. Additionally, a cryptographically-based pseudonym proxy server is provided to ensure the privacy of a user's target profile interest summary, by giving the user control over the ability of third parties to access this summary and to identify or contact the user.

Brief Summary Text (2):

This invention relates to customized electronic identification of desirable objects, such as news articles, in an electronic media environment, and in particular to a system that automatically constructs both a "target profile" for each target object in the electronic media based, for example, on the frequency with which each word appears in an article relative to its overall frequency of use in all articles, as well as a "target profile interest summary" for each user, which target profile interest summary describes the user's interest level in various types of target objects. The system then evaluates the target profiles against the users' target profile interest summaries to generate a user-customized rank ordered listing of target objects most likely to be of interest to each user so that the user can select from among these potentially relevant target objects, which were automatically selected by this system from the plethora of target objects that are profiled on the electronic media. Users' target profile interest summaries can be used to efficiently organize the distribution of information in a large scale system consisting of many users interconnected by means of a communication network. Additionally, a cryptographically based proxy server is provided to ensure the privacy of a user's target profile interest summary, by giving the user control over the ability of third parties to access this summary and to identify or contact the user.

Detailed Description Text (141):

The various processors interconnected by the data communication network N as shown in FIG. 1 can be divided into two classes and grouped as illustrated in FIG. 2: clients and servers. The clients C1-Cn are individual user's computer systems which are connected to servers S1-S5 at various times via data communications links. Each of the clients Ci is typically associated with a single server Sj, but with users can change over time. The clients C1-Cn both interface with users and produce and retrieve files to and from servers. The clients C1-Cn are not necessarily continuously on-line, since they typically serve a single user and can be movable systems, such as laptop

computers, which can be connected to the data communications network N at any of a number of locations. Clients could also be a variety of other computers, such as computers and kiosks providing access to customized information as well as targeted advertising to many users, where the users identify themselves with passwords or with smart cards. A server Si is a computer system that is presumed to be continuously on-line and functions to both collect files from various sources on the data communication network N for access by local clients C1-Cn and collect files from local clients C1-Cn for access by remote clients. The server Si is equipped with persistent storage, such as a magnetic disk data storage medium, and are interconnected with other servers via data communications links. The data communications links can be of arbitrary topology and architecture, and are described herein for the purpose of simplicity as point-to-point links or, more precisely, as virtual point-to-point links. The servers S1-S5 comprise the network vendors V1-Vk as well as the information servers I.sub.1 -I.sub.m of FIG. 1 and the functions performed by these two classes of modules can be merged to a greater or lesser extent in a single server Si or distributed over a number of servers in the data communication network N. Prior to proceeding with the description of the preferred embodiment of the invention, a number of terms are defined. FIG. 3 illustrates in block diagram form a representation of an arbitrarily selected network topology for a plurality of servers A-D, each of which is interconnected to at least one other server and typically also to a plurality of clients p-s. Servers A-D are interconnected by a collection of point to point data communications links, and server A is connected to client r, server B is connected to clients p-q, while server D is connected to client s. Servers transmit encrypted or unencrypted messages amongst themselves: a message typically contains the textual and/or graphic information stored in a particular file, and also contains data which describe the type and origin of this file, the name of the server that is supposed to receive the message, and the purpose for which the file contents are being transmitted. Some messages are not associated with any file, but are sent by one server to other servers for control reasons, for example to request transmission of a file or to announce the availability of a new file. Messages can be forwarded by a server to another server, as in the case where server A transmits a message to server D via a relay node of either server C or servers B, C. It is generally preferable to have multiple paths through the network, with each path being characterized by its performance capability and cost to enable the network N to optimize traffic routing.

Detailed Description Text (145):

Our method solves the above problems by combining the pseudonym granting and credential transfer methods taught by D. Chaum and J. H. Evertse, in the paper titled "A secure and privacy-protecting protocol for transmitting personal information between organizations," with the implementation of a set of one or more proxy servers distributed throughout the network N. Each proxy server, for example S2 in FIG. 2, is a server which communicates with clients and other servers S5 in the network either directly or through anonymizing mix paths as detailed in the paper by D. Chaum titled "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," published in Communications of the ACM, Volume 24, Number 2, February 1981. Any server in the network N may be configured to act as a proxy server in addition to its other functions. Each proxy server provides service to a set of users, which set is termed the "user base" of that proxy server. A given proxy server provides three sorts of service to each user U in its user base, as follows:

Detailed Description Text (151):

The service provider must have a means of protection from users who violate previously agreed upon terms of service. For example, if a user that uses a given pseudonym engages in activities that violate the terms of service, then the service provider should be able to take action against the user, such as denying the user service and blacklisting the user from transactions with other parties that the user might be tempted to defraud. This type of situation might occur when a user employs a service provider for illegal activities or defaults in payments to the service provider. The method of the paper titled "Security without identification: Transaction systems to make Big-Brother obsolete", published in the Communications of the ACM, 28(10), October 1985; pp. 1030-1044, incorporated herein, provides for a mechanism to enforce protection against this type of behavior through the use of resolution credentials, which are credentials that are periodically provided to individuals contingent upon their behaving consistent with the agreed upon terms of service between the user and information provider and network entities (such as regular payment for services rendered, civil conduct, etc.). For the user's safety, if the issuer of a resolution credential refuses to grant this resolution credential to the user, then the refusal may be appealed to an adjudicating third party. The integrity of the user profiles and target profile interest summaries stored on proxy servers is important: if a seller

relies on such user-specific information to deliver promotional offers or other material to a particular class of users, but not to other users, then the user-specific information must be accurate and untampered with in any way. The user may likewise wish to ensure that other parties not tamper with the user's user profile and target profile interest summary, since such modification could degrade the system's ability to match the user with the most appropriate target objects. This is done by providing for the user to apply digital signatures to the control messages sent by the user to the proxy server. Each pseudonym is paired with a public cryptographic key and a private cryptographic key, where the private key is known only to the user who holds that pseudonym; when the user sends a control message to a proxy server under a given pseudonym, the proxy server uses the pseudonym's public key to verify that the message has been digitally signed by someone who knows the pseudonym's private key. This prevents other parties from masquerading as the user.

Detailed Description Text (162):

In our system, the organizations that the user U interacts with are the servers S1-Sn on the network N. However, rather than directly corresponding with each server, the user employs a proxy server, e.g. S2, as an intermediary between the local server of the user's own client and the information provider or network vendor. Mix paths as described by D. Chaum in the paper titled "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communications of the ACM, Volume 24, Number 2, February 1981 allow for untraceability and security between the client, such as C3, and the proxy server, e.g. S2. Let $S(M,K)$ represent the digital signing of message M by modular exponentiation with key K as detailed in a paper by Rivest, R. L., Shamir, A., and Adleman, L. Titled "A method for obtaining digital signatures and public-key cryptosystems", published in the Comm. ACM 21, 2 February 120-126. Once a user applies to server Z for a pseudonym P and is granted a signed pseudonym signed with the private key SK.sub.z of server Z, the following protocol takes place to establish an entry for the user U in the proxy server S2's database D. 1. The user now sends proxy server S2 the pseudonym, which has been signed by Z to indicate the authenticity and uniqueness of the pseudonym. The user also generates a PK.sub.P, SK.sub.P key pair for use with the granted pseudonym, where is the private key associated with the pseudonym and PK.sub.p is the public key associated with the pseudonym. The user forms a request to establish pseudonym P on proxy server S2, by sending the signed pseudonym $S(P, SK.sub.z)$ to the proxy server S2 along with a request to create a new database entry, indexed by P, and the public key PK.sub.P. It envelopes the message and transmits it to a proxy server S2 through an anonymizing mix path, along with an anonymous return envelope header. 2. The proxy server S2 receives the database creation entry request and associated certified pseudonym message. The proxy server S2 checks to ensure that the requested pseudonym P is signed by server Z and if so grants the request and creates a database entry for the pseudonym, as well as storing the user's public key PK.sub.p to ensure that only the user U can make requests in the future using pseudonym P. 3. The structure of the user's database entry consists of a user profile as detailed herein, a target profile interest summary as detailed herein, and a Boolean combination of access control criteria as detailed below, along with the associated public key for the pseudonym P. 4. At any time after database entry for Pseudonym P is established, the user U may provide proxy server S2 with credentials on that pseudonym, provided by third parties, which credentials make certain assertions about that pseudonym. The proxy server may verify those credentials and make appropriate modifications to the user's profile as required by these credentials such as recording the user's new demographic status as an adult. It may also store those credentials, so that it can present them to service providers on the user's behalf.

Detailed Description Text (181):

In general, the user requests access to a particular target object or menu of target objects; once the corresponding file has been transmitted to the user's client processor, the user views its contents and makes another such request, and so on. Each request may take many seconds to satisfy, due to retrieval and transmission delays. However, to the extent that the sequence of requests is predictable, the system for customized electronic identification of desirable objects can respond more quickly to each request, by retrieving or starting to retrieve the appropriate files even before the user requests them. This early retrieval is termed "pre-fetching of files."

Detailed Description Text (189):

1. If proxy server S has not pre-fetched file Gi in the past t minutes, it retrieves file Gi and transmits it to user U's client processor q.

Detailed Description Text (220):

1. The proxy server S2 may restrict access by third parties to server S2's pseudonymous

database of user-specific information. When a third party such as an advertiser sends a message to server S2 requesting the release of user-specific information for a pseudonym P, server S2 refuses to honor the request unless the message includes credentials for the access or adequate to prove that the accessor is entitled to this information. The user associated with pseudonym P may at any time send signed control messages to proxy server S2, specifying the credentials or Boolean combinations of credentials that proxy server S2 should thenceforth consider to be adequate grounds for releasing a specified subset of the information associated with pseudonym P. Proxy server S2 stores these access criteria with its database record for pseudonym P. For example, a user might wish to proxy server S2 to release purchasing information only to selected information providers, to charitable organizations (that is, organizations that can provide a government-issued credential that is issued only to registered charities), and to market researchers who have paid user U for the right to study user U's purchasing habits.

Detailed Description Text (221):

2. The proxy server S2 may restrict the ability of third parties to send electronic messages to the user. When a third party such as an advertiser attempts to send information (such as a textual message or a request to enter into spoken or written real-time communication) to pseudonym P, by sending a message to proxy server S2 requesting proxy server S2 to forward the information to the user at pseudonym P, proxy server S2 will refuse to honor the request, unless the message includes credentials for the accessor adequate to meet the requirements the user has chosen to impose, as above, on third parties who wish to send information to the user. If the message does include adequate credentials, then proxy server S2 removes a single-use pseudonymous return address envelope from its database record for pseudonym P, and uses the envelope to send a message containing the specified information along a secure mix path to the user of pseudonym P. If the envelope being used is the only envelope stored for pseudonym P, or more generally if the supply of such envelopes is low, proxy server S2 adds a notation to this message before sending it, which notation indicates to the user's local server that it should send additional envelopes to proxy server S2 for future use.

Detailed Description Text (222):

In a more general variation, the user may instruct the proxy server S2 to impose more complex requirements on the granting of requests by third parties, not simply boolean combinations of required credentials. The user may impose any Boolean combination of simple requirements that may include, but are not limited to, the following:

Detailed Description Text (223):

(a.) the accessor (third party) is a particular party

Detailed Description Text (239):

1. The third party (accessor) transmits a request to proxy server S2 using the normal point-to-point connections provided by the network N. The request may be to access the target profile interest summaries associated with a set of pseudonyms P1 . . . Pn, or to access the user profiles associated with a set of pseudonyms P1 . . . Pn, or to forward a message to the users associated with pseudonyms P1 . . . Pn. The accessor may explicitly specify the pseudonyms P1 . . . Pn, or may ask that P1 . . . Pn be chosen to be the set of all pseudonyms registered with proxy server S2 that meet specified conditions.

Detailed Description Text (252):

We first show how to use the similarity-based methods described above to select the servers most interested in a group of target objects, herein termed "core servers" for that group. Next we show how to construct an unrooted multicast tree that can be used to broadcast files to these core servers. Finally, we show how files corresponding to target objects are actually broadcast through the multicast tree at the initiative of a client, and how these files are later retrieved from the core servers when clients request them.

Detailed Description Text (278):

In addition to global request messages, another type of message that may be transmitted to any proxy server S is termed a "query message." When transmitted to a proxy server, a query message causes a reply to be sent to the originator of the message; this reply will contain an answer to a given query Q if any of the servers in a given multicast tree MT(C) are able to answer it, and will otherwise indicate that no answer is available. The query and the cluster C are named in the query message. In addition, the query message contains a field S.sub.last which is unspecified except under certain

circumstances described below, when it names a specific core server. When a proxy server S receives a message M that is marked as a query message, it acts as follows: 1. Proxy server S sets A.sub.r to be the return address for the client or server that transmitted message M to server S. A.sub.r may be either a network address or a pseudonymous address 2. If proxy server S is not a core server for cluster C, it retrieves its locally stored list of nearby core servers for topic C, selects from this list a nearby core server S', and transmits a copy of the locate message M over a virtual point-to-point connection to core server S'. If this transmission fails, proxy server S repeats the procedure with other core servers on its list. Upon receiving a reply, it forwards this reply to address A.sub.r. 3. If proxy server S is a core server for cluster C, and it is able to answer query Q using locally stored information, then it transmits a "positive" reply to A.sub.r containing the answer. 4. If proxy server S is a core server for topic C, but it is unable to answer query Q using locally stored information, then it carries out a parallel depth-first search by executing the following steps: (a) Set L to be the empty list. (b) Retrieve the locally stored subtree of MT(C). For each server Si directly linked to S.sub.curr in this subtree, other than S.sub.last (if specified), add the ordered pair (Si S) to the list L. (c) If L is empty, transmit a "negative" reply to address A.sub.r saying that server S cannot locate an answer to query Q, and terminate the execution of step 4; otherwise proceed to step (d). (d) Select a list L1 of one or more server pairs (Ai, Bi) from the list L. For each server pair (Ai, Bi) on the list L1, form a locate message M(Ai, Bi), which is a copy of message M whose S.sub.last field has been modified to specify Bi, and transmit this message M(Ai, Bi) to server Ai over a virtual point-to-point connection. (e) For each reply received (by S) to a message sent in step (d), act as follows: (i) If a "positive" reply arrives to a locate message M(Ai, Bi), then forward this reply to A.sub.r and terminate step 4, immediately. (ii) If a "negative" reply arrives to a locate message M(Ai, Bi), then remove the pair (Ai, Bi) from the list L1. (iii) If the message M(Ai, Bi) could not be successfully delivered to Ai, then remove the pair (Ai, Bi) from the list L1, and add the pair (Ci, Ai) to the list L1 for each Ci other than Bi that is directly linked to Ai in the locally stored subtree of MT(C). (f) Once L1 no longer contains any pair (Ai, Bi) for which a message M(Ai, Bi) has been sent, or after a fixed period of time has elapsed, return to step (c).

Detailed Description Text (355):

With the help of the above procedure, and the multicast tree MT fill that includes all proxy servers in the network, the distributed hierarchical cluster tree for a particular domain of target objects is constructed by merging many local hierarchical cluster trees, as follows. 1. One server S (preferably one with good connectivity) is elected from the tree. 2. Server S sends itself a global request message that causes each proxy server in MT.sub.full (that is., each proxy server in the network) to ask its clients for files for the cluster tree. 3. The clients of each proxy server transmit to the proxy server any files that they maintain, which files represent target objects from the appropriate domain that should be added to the cluster tree. 4. Server S forms a request R1 that, upon receipt, will cause the recipient server S1 to take the following actions: (a) Build a hierarchical cluster tree of all the files stored on server S1 that are maintained by users in the user base of S1. These files correspond to target objects from the appropriate domain. This cluster tree is typically stored entirely on S1, but may in principle be stored in a distributed fashion. (b) Wait until all servers to which the server S1 has propagated request R have sent the recipient reply messages containing pointers to cluster trees. (c) Merge together the cluster tree created in step 5(a) and the cluster trees supplied in step 5(b), by sending any server (such as S1 itself) a message requesting such a merge, as described above. (d) Upon receiving a reply to the message sent in (c), which reply includes a pointer to a file representing the merged cluster tree, forward this reply to the sender of request R1, unless this is S1 itself. 5. Server S sends itself a global request message that causes all servers in MT.sub.full to act on embedded request R1. 6. Server S receives a reply to the message it sent in 5(c). This reply includes a pointer to a file F that represents the completed hierarchical cluster tree. Server S multicasts file F to all proxy servers in MT.sub.full. Once the hierarchical cluster tree has been created as above, server S can send additional messages through the cluster tree, to arrange that multicast trees MT(C) are created for sufficiently large clusters C, and that each file F is multicast to the tree MT(C), where C is the smallest cluster containing file F.

WEST

Generate Collection

Print

L8: Entry 10 of 12

File: USPT

DOCUMENT-IDENTIFIER: US 5694546 A

TITLE: System for automatic unattended electronic information transport between a server and a client by a vendor provided transport software with a manifest list

US PATENT NO. (1):5694546Brief Summary Text (13):

Recent press announcements from corporations such as AT&T, Lotus, Microsoft and MCI describe plans for new online services providing what are called "groupware" services to offer rich electronic mail and group collaboration functions, primarily for business organizations. Although offering multiple electronic object transport operations such services are believed to have complex setup procedures and software requirements and complex message routing features and protocols, and to lack interface flexibility. Accordingly, they are not suitable for mass distribution of low cost electronic information update products and cannot achieve the objectives of the invention.

Detailed Description Text (156):

Prospective publishers wishing to offer electronic products online, contract with online service providers to enable customers to use the online service's client software to access the publisher's material and related online communications services (bulletin boards, etc.) on the services' servers. The publisher is limited to using the presentation facilities provided by the user interface in the online service's client software. This limitation impedes migration of publisher offerings and makes it difficult for either a customer or a publisher to swing information transport component 14 access from one service provider to another because each service requires its own software package.

Detailed Description Text (157):

Third party interface developers cannot contribute to such online interfaces for a publisher without the cooperation of the online service provider which may be difficult or impossible to obtain. Accordingly, only limited user interfaces with moderate sophistication and variety can be offered.

Detailed Description Text (158):

Accordingly in another aspect, to provide open architecture online service communication, the inventive information transport component 14 can be embodied as a flexible client interface which can be actuated to operate with any one of a number of online services by providing a generic client interface foundation API (application program interface) combined with a set of translators and protocol drivers capable of communicating the user's functional requests to any one of a set of online services, using their corresponding proprietary protocols.

Detailed Description Text (159):

In this aspect the invention permits publishers to develop highly sophisticated and individualized user interfaces independently of the limitations of the online service providers' capabilities. Such enhanced user interfaces are attractive to publishers seeking differentiation of their products by providing an appealing individualized interface with a signature look and feel. In contrast, online service providers seeking to economically carry content from many publishers provide generic interfaces acceptable to all.

Detailed Description Text (189):

In addition to the benefits of a powerful and efficient information transport method, use of a standard, formalized transporter, its API, and client-server protocol, pursuant to the teachings of the invention disclosed herein, can provide any or all of

the following significant benefits to users, information product vendors, application vendors, service providers, tool vendors or others:

Detailed Description Text (207):

Level Three Adds a full online service user interface API with correspondingly enhanced client-server protocols to provide for full-function online service sessions with user interface control and with ability to work with a range of online services, providing a publisher with flexibility in their use of existing and emerging services.

WEST[Generate Collection](#)[Print](#)**Search Results - Record(s) 1 through 4 of 4 returned.**☐ 1. Document ID: US 5835087 A

L10: Entry 1 of 4

File: USPT

US-PAT-NO: 5835087

DOCUMENT-IDENTIFIER: US 5835087 A

TITLE: System for generation of object profiles for a system for customized electronic identification of desirable objects

Full	Title	Citation	Front	Review	Classification	Date	Reference	Sequences	Attachments	Claims	RWMC	Draw Desc	Image
------	-------	----------	-------	--------	----------------	------	-----------	-----------	-------------	--------	------	-----------	-------

☐ 2. Document ID: US 5754939 A

L10: Entry 2 of 4

File: USPT

US-PAT-NO: 5754939

DOCUMENT-IDENTIFIER: US 5754939 A

TITLE: System for generation of user profiles for a system for customized electronic identification of desirable objects

Full	Title	Citation	Front	Review	Classification	Date	Reference	Sequences	Attachments	Claims	RWMC	Draw Desc	Image
------	-------	----------	-------	--------	----------------	------	-----------	-----------	-------------	--------	------	-----------	-------

☐ 3. Document ID: US 5754938 A

L10: Entry 3 of 4

File: USPT

US-PAT-NO: 5754938

DOCUMENT-IDENTIFIER: US 5754938 A

TITLE: Pseudonymous server for system for customized electronic identification of desirable objects

Full	Title	Citation	Front	Review	Classification	Date	Reference	Sequences	Attachments	Claims	RWMC	Draw Desc	Image
------	-------	----------	-------	--------	----------------	------	-----------	-----------	-------------	--------	------	-----------	-------

☐ 4. Document ID: US 5722418 A

L10: Entry 4 of 4

File: USPT

US-PAT-NO: 5722418

DOCUMENT-IDENTIFIER: US 5722418 A

TITLE: Method for mediating social and behavioral processes in medicine and business through an interactive telecommunications guidance system

Full	Title	Citation	Front	Review	Classification	Date	Reference	Sequences	Attachments	Claims	RWMC	Draw Desc	Image
------	-------	----------	-------	--------	----------------	------	-----------	-----------	-------------	--------	------	-----------	-------

Generate Collection Print

Terms	Documents
L1 and (healthcare or health adj car\$3 or hospital or pharmac\$3 or food drug administration or FDA)	4

Display Format: TI Change Format

[Previous Page](#) [Next Page](#)

WEST

Generate Collection

Print

Search Results - Record(s) 1 through 12 of 12 returned.☐ 1. Document ID: US 5870724 A

L8: Entry 1 of 12

File: USPT

US-PAT-NO: 5870724

DOCUMENT-IDENTIFIER: US 5870724 A

TITLE: Targeting advertising in a home retail banking delivery service

Full	Title	Citation	Front	Review	Classification	Date	Reference	Sequences	Attachments
------	-------	----------	-------	--------	----------------	------	-----------	-----------	-------------

MM	Draw Desc	Image
----	-----------	-------

☐ 2. Document ID: US 5835087 A

L8: Entry 2 of 12

File: USPT

US-PAT-NO: 5835087

DOCUMENT-IDENTIFIER: US 5835087 A

TITLE: System for generation of object profiles for a system for customized electronic identification of desirable objects

Full	Title	Citation	Front	Review	Classification	Date	Reference	Sequences	Attachments
------	-------	----------	-------	--------	----------------	------	-----------	-----------	-------------

MM	Draw Desc	Image
----	-----------	-------

☐ 3. Document ID: US 5828837 A

L8: Entry 3 of 12

File: USPT

US-PAT-NO: 5828837

DOCUMENT-IDENTIFIER: US 5828837 A

TITLE: Computer network system and method for efficient information transfer

Full	Title	Citation	Front	Review	Classification	Date	Reference	Sequences	Attachments
------	-------	----------	-------	--------	----------------	------	-----------	-----------	-------------

MM	Draw Desc	Image
----	-----------	-------

☐ 4. Document ID: US 5802518 A

L8: Entry 4 of 12

File: USPT

US-PAT-NO: 5802518

DOCUMENT-IDENTIFIER: US 5802518 A

TITLE: Information delivery system and method

Full	Title	Citation	Front	Review	Classification	Date	Reference	Sequences	Attachments
------	-------	----------	-------	--------	----------------	------	-----------	-----------	-------------

MM	Draw Desc	Image
----	-----------	-------

☐ 5. Document ID: US 5778187 A

L8: Entry 5 of 12

File: USPT

US-PAT-NO: 5778187

DOCUMENT-IDENTIFIER: US 5778187 A

TITLE: Multicasting method and apparatus

Full	Title	Citation	Front	Review	Classification	Date	Reference	Sequences	Attachments
------	-------	----------	-------	--------	----------------	------	-----------	-----------	-------------

RMIC	Draw Desc	Image
------	-----------	-------

☐ 6. Document ID: US 5754939 A

L8: Entry 6 of 12

File: USPT

US-PAT-NO: 5754939

DOCUMENT-IDENTIFIER: US 5754939 A

TITLE: System for generation of user profiles for a system for customized electronic identification of desirable objects

Full	Title	Citation	Front	Review	Classification	Date	Reference	Sequences	Attachments
------	-------	----------	-------	--------	----------------	------	-----------	-----------	-------------

RMIC	Draw Desc	Image
------	-----------	-------

☐ 7. Document ID: US 5754938 A

L8: Entry 7 of 12

File: USPT

US-PAT-NO: 5754938

DOCUMENT-IDENTIFIER: US 5754938 A

TITLE: Pseudonymous server for system for customized electronic identification of desirable objects

Full	Title	Citation	Front	Review	Classification	Date	Reference	Sequences	Attachments
------	-------	----------	-------	--------	----------------	------	-----------	-----------	-------------

RMIC	Draw Desc	Image
------	-----------	-------

☐ 8. Document ID: US 5722418 A

L8: Entry 8 of 12

File: USPT

US-PAT-NO: 5722418

DOCUMENT-IDENTIFIER: US 5722418 A

TITLE: Method for mediating social and behavioral processes in medicine and business through an interactive telecommunications guidance system

Full	Title	Citation	Front	Review	Classification	Date	Reference	Sequences	Attachments
------	-------	----------	-------	--------	----------------	------	-----------	-----------	-------------

RMIC	Draw Desc	Image
------	-----------	-------

☐ 9. Document ID: US 5710884 A

L8: Entry 9 of 12

File: USPT

US-PAT-NO: 5710884

DOCUMENT-IDENTIFIER: US 5710884 A

TITLE: System for automatically updating personal profile server with updates to additional user information gathered from monitoring user's electronic consuming habits

generated on computer during use

Full	Title	Citation	Front	Review	Classification	Date	Reference	Sequences	Attachments
------	-------	----------	-------	--------	----------------	------	-----------	-----------	-------------

RMW	Draw Desc	Image
-----	-----------	-------

☐ 10. Document ID: US 5694546 A

L8: Entry 10 of 12

File: USPT

US-PAT-NO: 5694546

DOCUMENT-IDENTIFIER: US 5694546 A

TITLE: System for automatic unattended electronic information transport between a server and a client by a vendor provided transport software with a manifest list

Full	Title	Citation	Front	Review	Classification	Date	Reference	Sequences	Attachments
------	-------	----------	-------	--------	----------------	------	-----------	-----------	-------------

RMW	Draw Desc	Image
-----	-----------	-------

☐ 11. Document ID: US 5649186 A

L8: Entry 11 of 12

File: USPT

US-PAT-NO: 5649186

DOCUMENT-IDENTIFIER: US 5649186 A

TITLE: System and method for a computer-based dynamic information clipping service

Full	Title	Citation	Front	Review	Classification	Date	Reference	Sequences	Attachments
------	-------	----------	-------	--------	----------------	------	-----------	-----------	-------------

RMW	Draw Desc	Image
-----	-----------	-------

☐ 12. Document ID: US 5636346 A

L8: Entry 12 of 12

File: USPT

US-PAT-NO: 5636346

DOCUMENT-IDENTIFIER: US 5636346 A

TITLE: Method and system for selectively targeting advertisements and programming

Full	Title	Citation	Front	Review	Classification	Date	Reference	Sequences	Attachments
------	-------	----------	-------	--------	----------------	------	-----------	-----------	-------------

RMW	Draw Desc	Image
-----	-----------	-------

[Generate Collection](#)[Print](#)

Terms	Documents
11 and (healthcare or healt adj car\$3 or hospital or service adj provid\$3 or pharmac\$3 or food drug administration or FDA)	12

Display Format:[Change Format](#)[Previous Page](#)[Next Page](#)